REMARKS

Favorable reconsideration of this application is respectfully requested.

The specification is amended to correct minor informalities that are not believed to raise any new issues.

Claims 1-15 are pending in this application. Claims 1-15 were rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. patent 6,101,182 to Sistanizadeh et al. (herein "Sistanizadeh") in view of U.S. patent 6,826,690 to Hind et al. (herein "Hind"). That rejection is traversed as discussed next.

Initially, applicants note the claims are amended by the present response to clarify features recited therein. Specifically, the claims now clarify the transmission device and the reception device are "physically connected to an identical local area network, or are not physically connected to the identical local area network but virtually existing in an identical sub-net". The claims also now clarify that device identification information transmitted from a reception device is registered "by an upper level protocol above a network layer" and that device identification information corresponding to an IP address of the reception device is searched "by a protocol on the network layer".

The claimed invention is directed to distinguishing between a situation, and with reference to Figure 1 in the present specification as a non-limiting example, in which different devices, see for example sink device B, sink device C, and source device D, are all connected to the same local area network, but another device, such as the source device A, can also be virtually connected to that local area network. The present invention distinguishes between such cases to ensure, as a non-limiting example, that information from the source device D is only shared amongst other devices on the same local area network (e.g. sink devices B, C), but not with a virtually connected device such as source device A.

In view of the above operation, the claims now recite judging whether or not contents are transmitted to a target device by comparing a device identification information (as a non-limiting example a MAC address) transmitted by an upper level protocol above a network layer with a device identification information (in the non-limiting example the MAC address) transmitted by a protocol on a network layer. The features recited in the claims as currently written are believed to clearly distinguish over the applied art.

One object of the claimed invention is to provide a contents transmission/reception system, a contents transmission device, and a contents reception device capable of judging whether a transmission device and reception devices are physically connected to an identical local area network or are not physically connected to the identical local area network but are virtually existing in an identical sub-net, and then transmitting contents only to a reception device physically connected to the identical local area network (see e.g. the specification at page 3, line 11 - page 4, line 5; page 6, lines 6-14; page 8, line 15 - page 9, line 4; and FIGS. 33, 36).

To achieve the above object, the reception device (or the transmission device) has a function of sending to the transmission device (or the reception device) a device identification information by using an upper level protocol above a network layer. As a non-limiting example the device identification information can be a MAC address. Further, the transmission device (or the reception device) has a function of searching the device identification information (e.g. the MAC address) corresponding to an IP (Internet Protocol) address of the reception device (or the transmission device) by using the protocol (IP) on the network layer, and then comparing the sent device identification information with the searched device identification information.

The reception device and the transmission device can exchange the device identification information with each other by using the upper level protocol above the

network layer, regardless of whether or not they are existing in an identical segment on a network (e.g. Ethernet). In contrast, the reception device and the transmission device can not exchange the device identification information with each by using the protocol on the network layer if they are not existing in the identical segment on the network (e.g. Ethernet). Therefore, with the claimed invention it is possible to judge whether or not the reception device and the transmission device are physically connected in the identical segment on a network by comparing two pieces of device identification information of the reception device (or the transmission device) acquired by using two protocols belonging to different layers (see e.g. the specification at page 33, page 39, line 8; page 40, line 2-page 41, line 24; page 43, line 11 – page 41, line 5; page 44, line 24 – page 45, line 18; and FIGS. 1, 5-10).

In contrast to the claimed feature, Sistanizadeh discloses a system including a PC 710, a DHCP server 712, a DNS server 714 and a Host 716. The PC 710 carries out the following processes with the DHCP server 712 and the DNS server 714, to access to a desired provider (Host 716). The PC 710 sends a DHCP request to the DHCP server 712 so that the DHCP server 712 assigns an IP address to the PC 710. The DHCP server 712 sends to the PC 710 a Verification/Authentication regarding an authentication/key-exchange process when receiving the DHCP request. The PC 710 sends encrypted Login, Password, and MAC address to the DHCP server 712 when receiving the Verification/Authentication, and the DHCP server 712 identifies the desired provider of the PC 710 and sends to the PC 710 an IP address to be assigned to the PC 710 when receiving encrypted Login, Password, and MAC address. The PC 710 sends an IP Accept to the DHCP server 712 when receiving the IP address. The DHCP server 712 sends to the DNS server 714 a name of the PC 710 and the IP address assigned to the PC 710 to update the DNS server 714 when receiving the IP Accept. When the DNS server 714 sends a DNS Updated to the PC 710, the PC 710 learns an IP

address of the Host 716 from the DNS server 714 and then accesses the Host 716 (see col. 12 lines 3-46 and FIG. 7).

Therefore, Sistanizadeh fails to teach or suggest that the PC 710, the DHCP server 712, the DNS server 714 or the Host 716 judge whether or not contents are transmitted to a target device by comparing a device identification information (as a non-limiting example a MAC address) transmitted by an upper level protocol above a network layer with a device identification information transmitted by a protocol on the network layer.

Further, Hind cannot cure the deficiencies in Sistanizadeh. Hind discloses a method for authenticating a device prior to automatically and dynamically assigning an IP address to the device. The method of Hind includes: (1) a storage in which a device's private key is securely stored is added to a device's LAN adapter card and then the adapter card is physically installed in the server; (2) a public key/private key pair and a device certificate are created for the device and the device certificate includes a unique device identifier and the device's public key; (3) the device generates a digital signature on a request command including the device certificate by using the device's private key and then transmits the request command to the server; (4) the server authenticates the transmitted request command by using the device's public key prior to assigning an IP address; and (5) the server judges whether or not a unique device identifier stored in the adapter card is identical to the unique device identifier included in the device certificate when the authentication of the request command is valid (see Hind at col. 12, line 58 - col. 15, line 10; col. 17, line 63 - col. 18, line 27; and FIG. 7A).

Therefore, Hind also fails to teach or suggest that the server judges whether or not contents are transmitted to the device by comparing a device identification information (e.g. unique device identifier) transmitted by an upper level protocol above a network layer with a

device identification information (e.g., unique device identifier) transmitted by a protocol on the network layer. Thus, Hind cannot cure the deficiencies in Sistanizadeh.

In view of these foregoing comments, applicants respectfully submit the claims as currently written clearly distinguish over Sistanizadeh in view of Hind.

As no other issues are pending in this application, it is respectfully submitted that the present application is now in condition for allowance, and it is hereby respectfully requested that this case be passed to issue.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870

Surinder Sachar
Registration No. 34,423

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

EHK/SNS/law
I:\ATTY\SNS\24'S\246433\246433US-AM.DOC